(19) **RU** (11) **2 220 447** (13) **C2**

(51) Int. Cl.[7] **G 06 F 15/16, 12/14, H 04 L 29/06**

RUSSIAN AGENCY
FOR PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: 2000100930/09, 09.04.1998

(24) Effective date for property rights: 09.04.1998

(30) Priority: 16.06.1997 DE 19725444.6

(43) Application published: 20.12.2001

(46) Date of publication: 27.12.2003

(85) Commencement of national phase: 16.01.2000

(86) PCT application:
DE 98/01043 (09.04.1998)

(87) PCT publication:
WO 98/58304 (23.12.1998)

(98) Mail address:
129010, Moskva, ul. B. Spasskaja, 25, str.3,
OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. Ju.D.Kuznetsovu, reg.№ 595

(72) Inventor: POKRANDT Vol'fgang (DE)

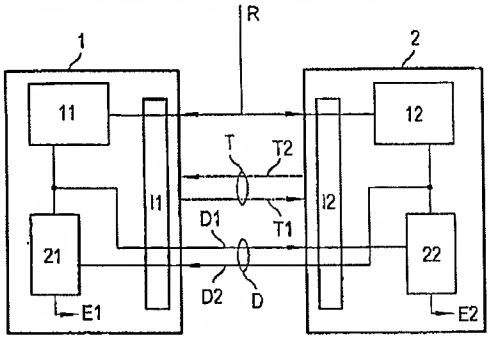
(73) Proprietor:
INFINEON TEKNOLODZhIZ AG (DE)

(74) Representative:
Kuznetsov Jurij Dmitrievich

(54) AUTHORIZATION CHECK METHOD AND CIRCUIT THEREOF

(57) Abstract:

FIELD: data exchange devices incorporating authorization provision. SUBSTANCE: check data are generated in each of two data exchange devices around starting signal and transferred from one data exchange device to other; data obtained are compared with check data of data exchange device that has received these data and decision is taken to authorize data exchange basing on comparison results; one of two data exchange devices specifies one common time step and informs other device that it has taken control functions. Circuit implementing this method has data exchange devices, starting signal supply device, interface for data receiving and transmitting, and data processing device incorporating comparator. EFFECT: enhanced obstruction in keyword detection. 8 cl, 5 dwg



Фиг.1

RU 2220447 C2

RU 2220447 C2

(19) RU (11) 2 220 447 (13) C2

(51) МПК7 G 06 F 15/16, 12/14, H 04 L 29/06

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21), (22) Заявка: 2000100930/09, 09.04.1998

(24) Дата начала действия патента: 09.04.1998

(30) Приоритет: 16.06.1997 DE 19725444.6

(43) Дата публикации заявки: 20.12.2001

(46) Дата публикации: 27.12.2003

(56) Ссылки: DE 4328781 A1, 02.03.1995. RU 2080652 C1, 27.05.1997. EP 0636963 A2, 01.02.1995. US 4885778 A, 05.12.1989. RU 2020565 C1, 30.09.1994.

(85) Дата перевода заявки PCT на национальную фазу: 16.01.2000

(86) Заявка PCT:
DE 98/01043 (09.04.1998)

(87) Публикация PCT:
WO 98/58304 (23.12.1998)

(98) Адрес для переписки:
129010, Москва, ул. Б. Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(72) Изобретатель: ПОКРАНДТ Вольфганг (DE)

(73) Патентообладатель:
ИНФИНЕОН ТЕКНОЛОДЖИЗ АГ (DE)

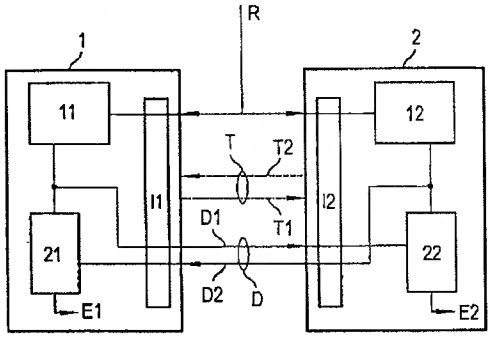
(74) Патентный поверенный:
Кузнецов Юрий Дмитриевич

RU 2220447 C2

(54) СПОСОБ ПРОВЕРКИ РАЗРЕШЕНИЯ И СХЕМА ДЛЯ ОСУЩЕСТВЛЕНИЯ ЭТОГО СПОСОБА

(57)

Изобретение относится к устройствам обмена данными с установлением разрешения на обмен данными. Техническим результатом является создание способа и устройства, при которых в высокой степени затруднено обнаружение ключевого слова. Для этого на основе пускового сигнала в каждом из двух устройств обработки данных вырабатываются проверочные данные, которые передаются от одного устройства обработки данных к другому, полученные данные сравниваются с проверочными данными устройства обработки данных, которое получило эти данные, и на основе результатов сравнения принимается решение на разрешение обмена данными, при этом одно из двух устройств обработки данных задает один общий такт и сообщает другому устройству о взятии на себя функции управления. Схема содержит устройства обработки данных, устройство подачи пускового сигнала, интерфейс для приема и передачи данных, устройство обработки данных содержит компаратор. 2 с. и 6 з.п.ф-лы, 5 ил.



Фиг.1

RU 2220447 C2

Изобретение относится к способу проверки наличия разрешения на обмен между собой данными, по меньшей мере, двух связанных между собой устройств обработки данных и к схеме для осуществления этого способа. Обмен данными между двумя и более устройствами обработки данных сегодня является обычной процедурой. При этом все большее значение приобретает вопрос о том, имеют ли связанные между собой устройства обработки данных разрешение на обмен данными вообще или на обмен определенными данными. Подобная проверка всегда необходима в тех случаях, когда имеющаяся в устройстве обработки данных информация должна быть доступна только определенному кругу лиц или имеющиеся в нем данные должны быть доступны отведенным этому кругу лиц устройствам обработки данных.

Обычно эту проверку проводят путем обмена кодовыми или ключевыми словами, позволяющими подтвердить разрешение. Проблему этого обычного метода следует усматривать в том, что при проверке канала передачи данных кодовое слово при его регулярном употреблении можно узнать. Кроме того, существует опасность того, что, если ключевое слово хранится, по меньшей мере, в одном устройстве обработки данных, то его можно легко узнать. В обоих случаях существует опасность неправомерного использования ключевого слова и, тем самым, несанкционированного доступа к информации.

В основе изобретения лежит поэтому задача создания способа и схемы для применения этого способа, при котором в более высокой степени затруднено обнаружение ключевого слова.

Эта задача решается согласно изобретению посредством признаков, приведенных в п.п. 1 и 8 формулы изобретения.

За счет того что в устройствах обработки данных, предусмотренных для обмена данными, проверочные данные хранят не постоянно, а вырабатывают каждый раз заново перед обменом данными, постоянно хранимое ключевое слово узнать невозможно. За счет того что невозможно также перед каждой передачей данных выработать другие проверочные данные, в более высокой степени затруднено также обнаружение проверочных данных при проверке канала передачи данных.

Другие предпочтительные формы выполнения изобретения приведены в зависимых пунктах формулы. За счет того, что при одновременной подаче пускового сигнала к предусмотренным для передачи данных устройствам обработки данных существует возможность, что либо тот, кто первым принял пусковой сигнал, либо первым выработал проверочные данные, или что по другой избирательной схеме определено, кто передает проверочные данные для проверки и кто принимает их, невозможно непосредственно предугадать, в какой момент времени от какого устройства обработки данных к какому передаются проверочные данные. Кроме того, существует возможность затруднить обнаружение проверочных данных путем их зашифровки. В любом случае предусмотрено, что в одном из устройств обработки данных проверочные данные сравнивают между собой и в зависимости от результата проверки принимают решение, допустим ли обмен данными или нет.

Изобретение более подробно поясняется ниже с помощью примеров выполнения со ссылкой на чертежи, на которых изображают:

- фиг.1: принципиальную структуру схемы согласно изобретению;
- фиг. 2-4: более подробный пример выполнения с несколькими вариантами;
- фиг.5: второй пример выполнения, согласно изобретению.

С помощью фиг.1 прежде всего следует пояснить основной принцип способа согласно изобретению и основную структуру схемы согласно изобретению.

Ссылочными позициями 1 и 2 обозначены два устройства обработки данных, имеющих функционально соответствующую структуру. Каждое из обоих устройств обработки данных располагает интерфейсом I1, I2, через которые принимают и/или передают данные или информацию. Далее предусмотрен генератор 11, 12 данных, в котором вырабатываются проверочные данные. Наконец, предусмотрен компаратор 21, 22, сравнивающий проверочные данные.

Пусковой или инициализирующий сигнал R подают в этом примере выполнения к обоим устройствам 1, 2 обработки данных. По этому пусковому сигналу R, подаваемому через интерфейс I1 к генератору 11, последний вырабатывает проверочные данные. Поскольку пусковой сигнал R подают одновременно через интерфейс I2 к генератору 12 в устройстве 2, он вырабатывает проверочные данные одновременно с генератором 11 в устройстве 1. Проверочные данные, вырабатываемые генератором в устройстве 1, передают через интерфейс I1 в качестве проверочных данных D1 к устройству 2, где компаратор 22 сравнивает их с проверочными данными, выработанными генератором 12. На основе результата сравнения компаратор 22 выдает выходной сигнал E2, показывающий, допустим ли обмен данными с устройством 1. В то же время выработанные в устройстве 2 проверочные данные передают к устройству 1, где их через интерфейс I1 принимают в качестве проверочных данных D2 и подают к компаратору 21. В компараторе 21 соответственно компаратору 22 проверочные данные, выработанные в генераторе 11, сравнивают с проверочными данными D1. В соответствии с результатом сравнения посредством компаратора 21 вырабатывают сигнал E1, показывающий, допустим ли обмен данными или нет.

Хотя в этом примере выполнения по фиг.1 структура обоих устройств 1 и 2 является функционально соответствующей, идентичная параллельная структура необязательна. Может быть, например, предусмотрено, что тот, кто первым принимает пусковой сигнал R, всегда передает проверочные данные к другому устройству обработки данных для их проверки. В равной мере может быть предусмотрено, что в устройстве обработки данных, которое первым принимает пусковой сигнал R, происходит сравнение проверочных данных. Точно так же можно использовать этот критерий выбора для того, чтобы определить, какое устройство обработки

RU 2220447 C2

RU 2220447 C2

данных первым выработало или первым приняло проверочные данные. Наконец, возможно, чтобы одно из обоих устройств обработки данных постоянно отвечало за сравнение проверочных данных. В этом случае канал D передачи проверочных данных должен быть выполнен не двунаправленным, а для передачи проверочных данных только в одном направлении. Наконец, возможно еще сравнение проверочных данных по определенной схеме чередования либо устройством 21, либо устройством 22.

Во всех случаях может быть предпочтительным предусмотреть тактовый передающий канал T, по которому от устройства 1 к устройству 2 передают тактовый сигнал T1 и/или от устройства 2 к устройству 1 передают тактовый сигнал T2.

На фиг.2 более подробно изображена принципиальная схема, изображенная на фиг. 1. Здесь также предусмотрены устройства 1 и 2 обработки данных. К ним подают пусковой сигнал R.

Также в этом примере выполнения схемы обоих устройств 1 и 2 являются функционально соответствующими. После подачи пускового сигнала R, например, устройство 1 приобретает функцию управления и передает такт T, вырабатываемый тактовым генератором 31. С управлением от такта в обеих активирующих логических схемах 41, 42 обоих устройств 1, 2 синхронно отрабатывается циклическая программа, а результате чего в обоих устройствах 1, 2 вырабатываются сигналы P1, P2 и S3. Сигнал S3 управляет в устройстве 1 тактовой частотой тактового генератора 31. Далее сигналы P1, P2 вместе с тактовым сигналом T управляют зарядным состоянием конденсатора C1. Помимо того, что постоянно задано, что устройство 1 обладает функцией управления, это согласование может происходить за счет подачи управляющего сигнала S5 к каждой активирующей логической схеме 41, 42 в обоих устройствах 1, 2. При этом установление происходит так, как это пояснялось, например, со ссылкой на фиг.1. В качестве опции этого установления предусмотрена передача активирующего сигнала A, с помощью которого одно из обоих устройств 1, 2 сообщает соответственно другому о том, что оно взяло на себя функцию управления. В любом случае приняты подходящие меры, которые препятствуют тому, чтобы оба устройства 1, 2 брали на себя функцию управления, что неизбежно привело бы к работе с ошибками.

Как уже сказано, необходимо установить, что устройство 1 взяло на себя функцию управления. Для того чтобы предотвратить теперь легкое обнаружение проверочных данных, от устройства 2 к устройству 1 передают случайные данные в качестве проверочных данных D. В это время конденсаторы C1, C2 в обоих устройствах 1, 2 одновременно заряжают и в определенный момент запрашивают. При этом момент запроса либо твердо задан, и он протекает в зависимости от тактовой частоты, либо его устанавливают посредством передачи активирующего сигнала A от одного из обоих устройств 1, 2. С управлением от сигнала S4 значение напряжения конденсаторов C1, C2 преобразуется через аналого-цифровые преобразователи AD1, AD2 в цифровое числовое значение. При этом аналого-цифровой преобразователь AD1 подает преобразованное а цифровую форму значение напряжения конденсатора C1 к компаратору 21, тогда как аналого-цифровой преобразователь AD2 передает преобразованное в цифровую форму значение напряжения конденсатора C1 через переключатель SW2 устройства 2 к устройству 1. Здесь переданные данные D, принятые в качестве проверочных данных, подаются через коммутирующее устройство SW1 к компаратору 21. Этот компаратор 21 проверяет и те, и другие проверочные данные и устанавливает, имеется ли разрешение на дальнейший обмен данными. Разрешение не обязательно должно зависеть от равенства или идентичности сравненных проверочных данных. Возможна также любая функциональная связь между проверочными данными. Целесообразными являются, однако, лишь такие связи, которые допускают однозначное суждение.

На фиг.3 изображен еще один вариант примера выполнения, причем одинаковые элементы обозначены теми же ссылочными позициями. Существенное отличие от изображенной на фиг.2 схемы состоит в том, что преобразованное в аналого-цифровом преобразователе AD1, AD2 значение напряжения конденсатора C1, C2 связывают в схеме V1, V2 связи с кодовым словом из памяти SP1, SP2 кодовых слов для его подачи затем к одному из компараторов 21, 22.

Изображенный на фиг.4 вариант отличается от изображенного на фиг.3 варианта тем, что в устройстве 2 обработки данных предусмотрен счетчик VZ попыток, который подсчитывает число попыток для достижения допуска к обмену данными. При превышении заданного числа управляющий сигнал P1 блокирует активирующую логическую схему 42. Этот счетчик VZ попыток может быть сброшен только при успешной попытке.

У изображенного на фиг.5 примера выполнения показан еще один пример вырабатывания проверочных данных. Также здесь предусмотрено два устройства 1, 2 обработки данных аналогичной структуры. Согласно одной из описанных выше возможностей, необходимо установись, что устройство 1 обладает функцией управления. При этом в памяти SP ключевых слов хранится ключевое слово. Оно простирается по заданному числу n областей памяти, запрашиваемых через адресные шины Am1, Am2-Amn и считываемых в сравнивающую или вычислительную логическую схему VL. Здесь сегмент ключевого слова или несколько сегментов, составленных в новое ключевое слово, направляют дальше к устройству 1, причем в сравнивающей или вычислительной логической схеме VL может осуществляться кодирование выработанных таким образом проверочных данных. В устройстве 1 в соответствующей сравнивающей или вычислительной логической схеме происходит затем сравнение с соответственно выработанными проверочными данными.

Как показано на фиг.5, управление адресными шинами Am1-Amn происходит

RU 2220447 C2

RU 2220447 C2

таким образом, что в результате передачи одного такта T приводится в действие адресный счетчик, указывающий на выходах Ad1-Adn адрес, который посредством подаваемого управляющего сигнала S изображенной избирательной схемы манипулирует адресом адресного счетчика.

Изображенная манипулирующая схема может быть произвольно изменена, причем адресом можно манипулировать с помощью произвольной логической схемы. Кроме того, предпочтительным образом управляющий сигнал вырабатывается в устройстве 1 генератором случайных чисел.

В заключение следует еще указать на то, что пример выполнения на фиг.5 может быть комбинирован в любой реализуемой форме с примером выполнения на фиг. 2-4. Также предусмотрено, что пусковой сигнал выдается одним из устройств 1, 2 обработки данных и что функция управления может перейти от одного из устройств обработки данных к соответственно другому.

Формула изобретения:

1. Способ проверки наличия разрешения на обмен данными между собой, по меньшей мере, двух связанных друг с другом устройств (1, 2) обработки данных, при котором на основе пускового сигнала в каждом из двух устройств (1, 2) обработки данных вырабатывают проверочные данные, к одному из, по меньшей мере, двух устройств (1, 2) обработки данных передают проверочные данные от, по меньшей мере, одного другого устройства обработки данных, в одном устройстве обработки данных выработанные в этом устройстве обработки данных проверочные данные сравнивают с проверочными данными, переданными к этому устройству обработки данных, на основе сравнения проверочных данных принимают решение, имеется ли разрешение на обмен данными, по меньшей мере, между двумя устройствами обработки данных, отличающийся тем, что одно из двух устройств обработки данных задает один общий такт для двух устройств обработки данных и что предусматривают передачу активирующего сигнала, с помощью которого одно из двух устройств обработки данных сообщает соответственно другому о том, что оно взяло на себя функцию управления.

2. Способ по п.1, при котором пусковой сигнал одновременно подают, по меньшей мере, к двум устройствам (1, 2) обработки данных.

3. Способ по п.1 или 2, при котором одно из, по меньшей мере, двух устройств (1, 2) обработки данных принимает пусковой сигнал первым.

4. Способ по одному из пп.1-3, при котором предварительно определяют, в каком из, по меньшей мере, двух устройств (1, 2) обработки данных происходит сравнение проверочных данных.

5. Способ по п.4, при котором определение, в каком из, по меньшей мере, двух устройств (1, 2) обработки данных происходит сравнение проверочных данных, осуществляют в зависимости от того, в каком из, по меньшей мере, двух устройств (1, 2) обработки данных проверочные данные вырабатывают первыми.

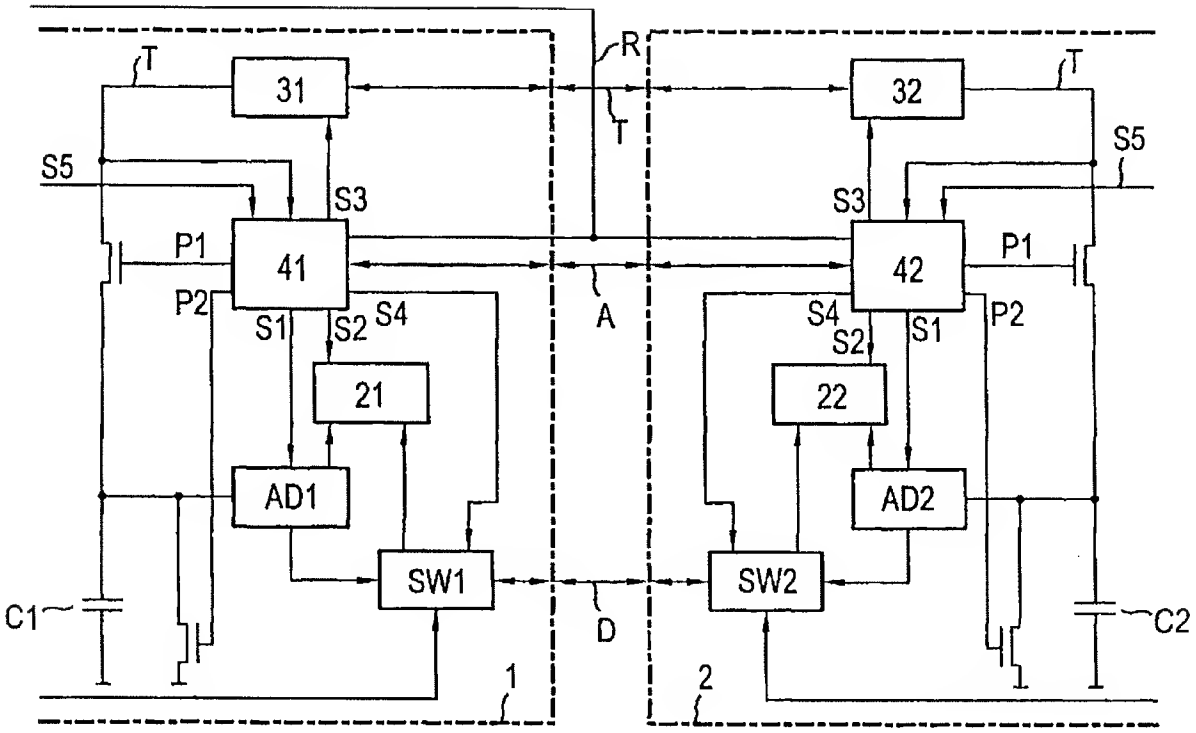
6. Способ по одному из пп.1-5, при котором проверочные данные передают в зашифрованном виде.

7. Способ по п.6, при котором зашифрованные проверочные данные сравнивают.

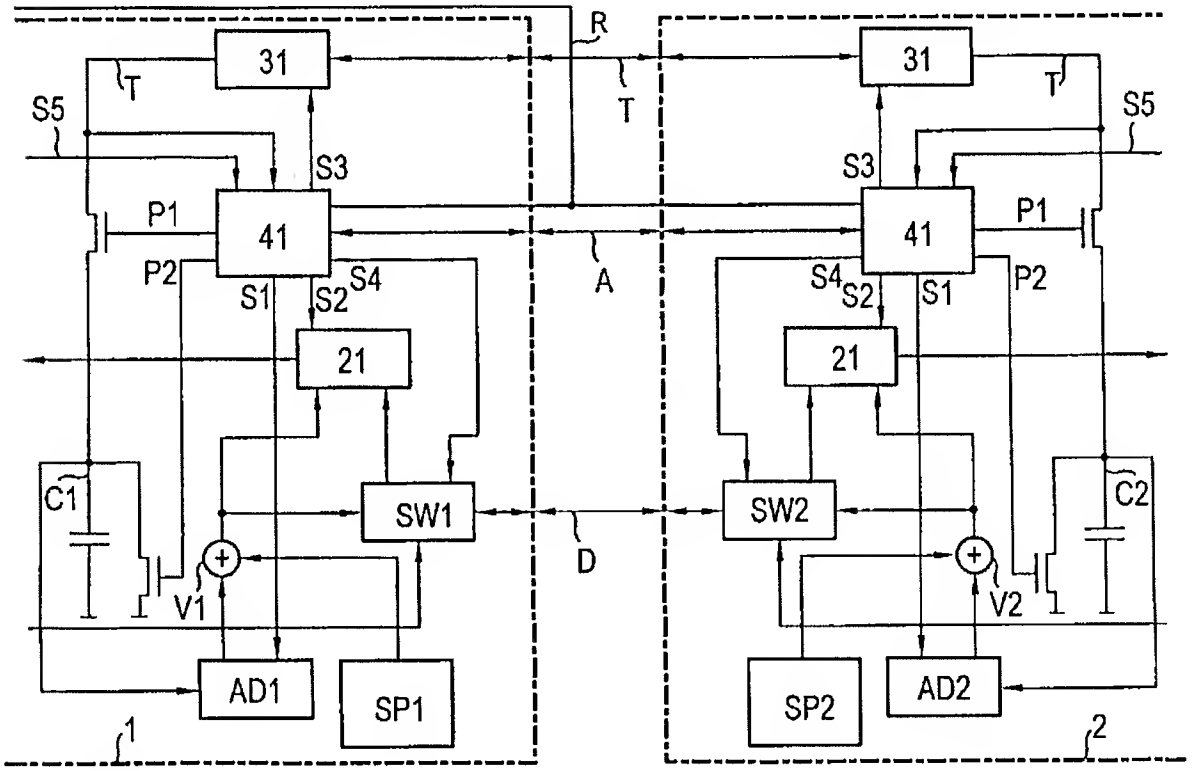
8. Схема для осуществления способа по п.1, содержащая, по меньшей мере, два устройства (1, 2) обработки данных и устройство для подачи пускового сигнала, причем все устройства (1, 2) обработки данных содержат генератор (11, 12) данных, который на основе подаваемого пускового сигнала вырабатывает проверочные данные, и интерфейс (11, 12) для приема и передачи данных, при этом одно, по меньшей мере, из двух устройств (1, 2) обработки данных содержит компаратор (21, 22) для сравнения выработанных проверочных данных с принятыми через интерфейс (11, 12) проверочными данными другого, по меньшей мере, из двух устройств (1, 2) обработки данных и для подачи сигнала сравнения, причем предусмотрена передача активирующего сигнала, с помощью которого одно из обоих устройств (1, 2) обработки данных сообщает соответственно другому о том, что оно взяло на себя функцию управления.

RU 2220447 C2

RU 2220447 C2



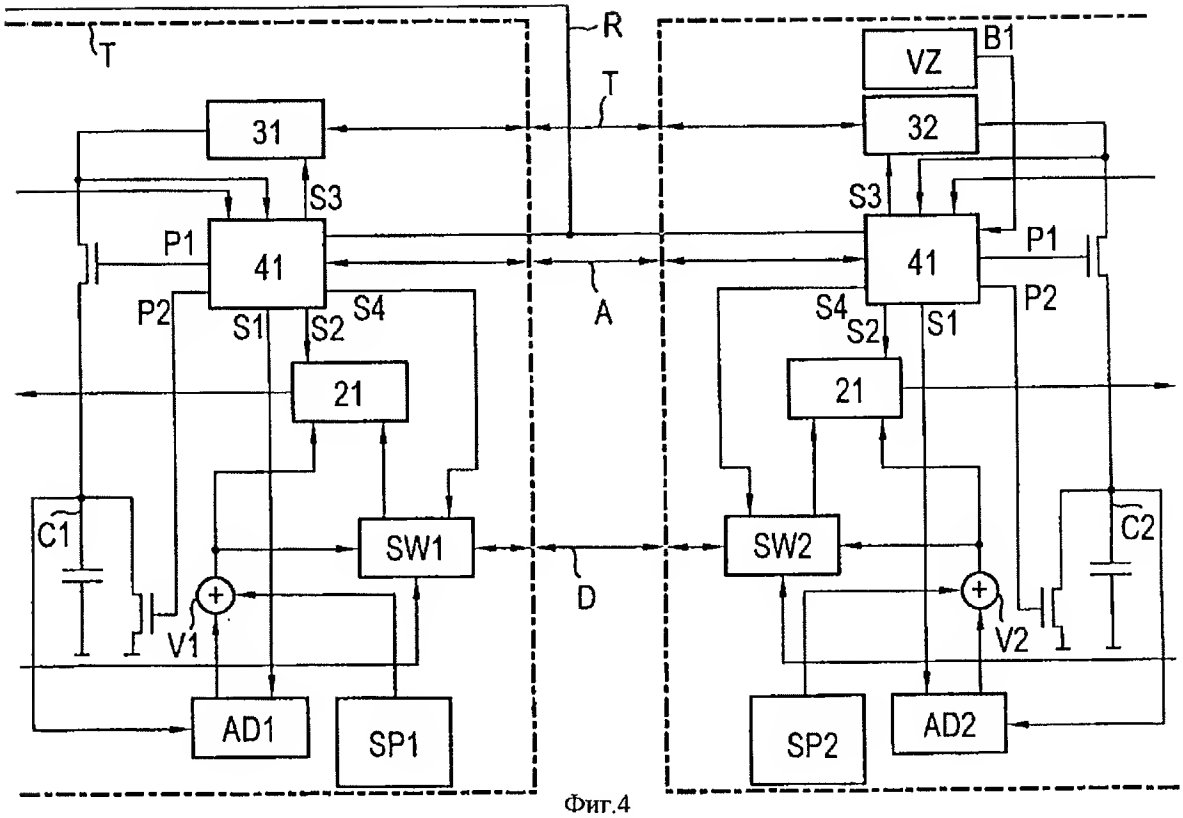
Фиг.2



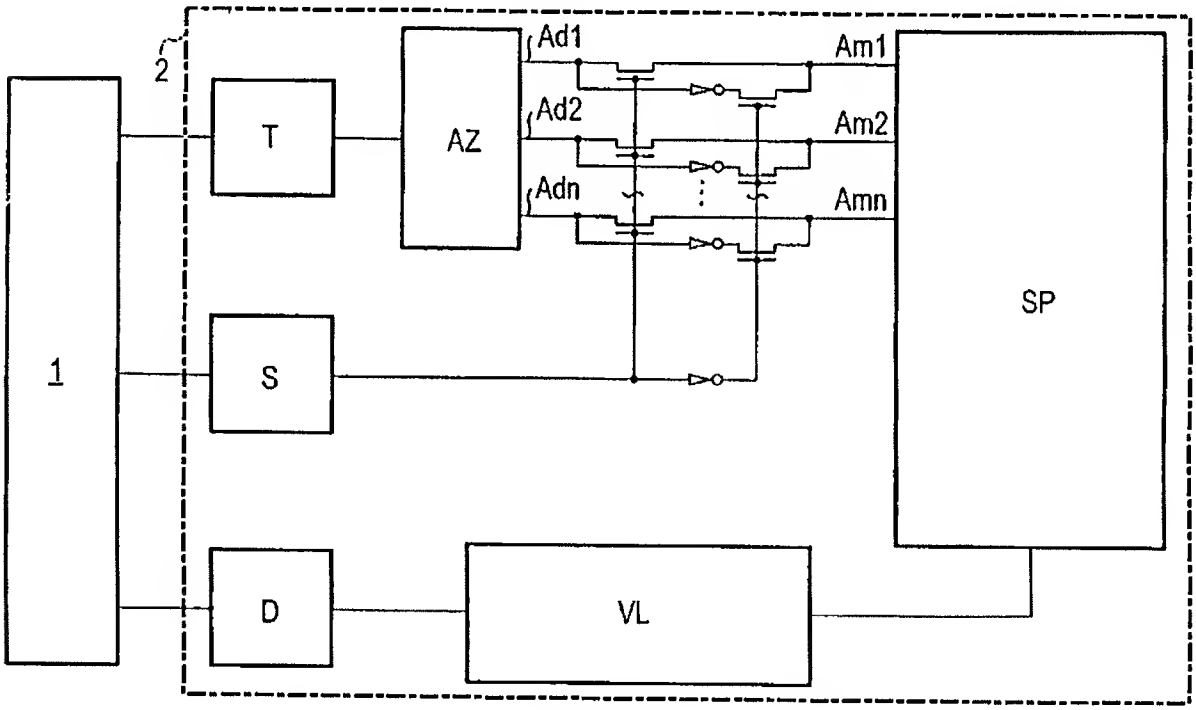
Фиг.3

RU 2220447 C2

RU 2220447 C2



Фиг.4



Фиг.5

RU 2220447 C2

RU 2220447 C2